AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the
District of Delaware

SEALED

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

APPLE ICLOUD ACCOUNT, APPLE ICLOUD BACKUP DATA, APPLE MACBOOK PRO LAPTOP F/N FVFVC2MMHV2G, AND A WESTERN DITIGAL HARD DRIVE S/N WX2IA19ATFF3

Case No. 23- 307M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein.

located in the _____ District of Delaware , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein.

FILED

DEC - 4 2023

U.S. DISTRICT COURT DISTRICT OF DELAWARE

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 922(a)(6)	Making A False Statement During a Background Check
18 U.S.C. § 924(a)(1)(A)	Making A False Statement on Records that Firearms Dealer is Required to Maintain
18 U.S.C. § 922(g)(3)	Illegal Possession of a Firearm

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet

[redacted]
Applicant's signature

[redacted]
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: December 4, 2023

Christopher J. Burke
Judge's signature

City and state: Wilmington, Delaware

Hon. Christopher J. Burke, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF: APPLE ICLOUD ACCOUNT, APPLE ICLOUD BACKUP DATA, APPLE MACBOOK PRO LAPTOP S/N FVFXC2MMHV2G, and a WESTERN DIGITAL EXTERNAL HARD DRIVE S/N WX2IA19ATFF3	Case No. 23-507M

AFFIDAVIT IN SUPPORT OF
AN APPLICATION UNDER RULE 41 FOR
A WARRANT TO SEARCH AND SEIZE

I [redacted] being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of:

   a. Information associated with Apple Inc. email address <rhbdc@icloud.com>, (hereafter the "APPLE ICLOUD ACCOUNT");

   b. the following backups produced by Apple on September 25, 2019:

      i. A backup of Apple iPhone X Device Identification D_8c78970d9dda9f5dbc1625b311efc72a6c50f68f ("Apple Backup 1");
      ii. A backup of Apple iPhone 6S Device Identification D_cdbe6900fc533da66a6c28169158d05cfb419a70 ("Apple Backup 3");
      iii. A backup of Apple iPad Pro Device Identification D_f846713a36c06653457179e18582aa1c478e8db4 ("Apple Backup 4"); and
      iv. A backup of Apple iPhone XR Device Identification D_a15b4a173b8ee009ee9adb908be74e4db618a323 ("Apple Backup 11").

(hereafter collectively identified as the "APPLE ICLOUD BACKUP DATA");

c. Apple MacBook Pro Laptop Computer; Serial Number FVFXC2MMHV29 (hereinafter "MACBOOK PRO"); and a

d. Western Digital External Hard Drive; Serial Number WX21A19ATFF3 (hereinafter "EXTERNAL HARD DRIVE")

all of which are more fully described in Attachment A and are currently located at the FBI-Wilmington Resident Agency, 500 Delaware Avenue, Suite 300 Wilmington, Delaware, 19801.

2. I request the authority to conduct the extraction from this property of the kind of electronically stored information described in Attachment B.

3. As described in detail in paragraph 22, the Government requests authorization to search for evidence of firearms related violations.

4. I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

5. I am a duly sworn member of the Federal Bureau of Investigation ("FBI") and have been so employed since March 2018. I am currently assigned to the Baltimore Field Office of the FBI, in Wilmington, Delaware. I participated in new agent training at the FBI Academy in Quantico, Virginia, which included training on drug and firearms offenses. I have successfully completed in-service training courses on drug enforcement sponsored by the FBI, Drug Enforcement Administration ("DEA"), and the United States Department of Justice. While employed by the FBI, I have investigated federal criminal violations related to gangs, bank robbery, narcotics offenses, firearms offenses, kidnapping, and fugitives.

6. Since July 2018, I have been assigned to the FBI's Delaware Violent Crimes/Safe Streets Task Force, which investigates violations of federal drug and firearms statutes. I am responsible for investigations involving unlawful activities to include drug smuggling/trafficking, firearms offenses and violent crime occurring in the District of Delaware.

7. I have actively participated in investigations of criminal activity, including but not limited to the investigation of narcotics offenses. During these investigations, I have also participated in the execution of search warrants and the seizure of evidence relating to drug activities. As a Special Agent of the FBI, I have testified under oath, affirmed applications of search and arrest warrants, and conducted and participated in Title III wire intercept investigations for the enforcement of federal laws. As a Special Agent of the FBI, I have personally conducted, supervised, and participated in investigations which have resulted in the arrest and convictions of numerous individuals responsible for narcotics offenses and firearms offenses.

8. I have also been involved in Organized Crime Drug Enforcement Task Force investigations involving drug organizations. As a result of this and other narcotics-related investigations, I have experience in debriefing defendants, informants, participants and various persons with direct experience with the methods used to purchase and distribute controlled substances.

9. Based on my training and experience as a Special Agent of the FBI, I am familiar with the means and methods that narcotics offenders use to import, distribute and purchase illicit drugs. I have become knowledgeable about the criminal statutes of the United States, particularly the criminal laws relating to violations of the federal narcotics, firearms, and conspiracy statutes.

10. The facts in this affidavit come from my personal observations, my review of subpoenaed and other records and evidence, my training and experience, and information obtained

from other members of law enforcement and witnesses. This affidavit is intended to show merely that sufficient probable cause for a search warrant but does not set forth all of my knowledge about this matter.

II. IDENTIFICATION OF THE EVIDENCE AND DEVICES TO BE EXAMINED

A. APPLE ICLOUD ACCOUNT AND APPLE ICLOUD BACKUP DATA

11. According to Apple.com, the "iCloud" is a paid service that allows a user to store their photos, videos, documents, music, and applications. In addition, the user can also save and store backups of their Apple products, to include iPhones, iPads and iMacs.

12. According to records provided by Apple, <rhbdc@icloud.com> was created on or about October 17, 2011, in the name of the HUNTER BIDEN.

13. This Court issued a search warrant for "information associated with Apple Inc. email address <rhbdc@icloud.com>," that was stored at Apple, Inc. in August 2019 for evidence of tax violations. *See* District of Delaware Case Number 19-234 M, issued on August 29, 2019.

14. In response to the Court's search warrant, on or about September 25, 2019, Apple provided investigators with production 19275210. This production included both the contents of the APPLE ICLOUD ACCOUNT and APPLE ICLOUD BACKUP DATA for a number of devices.[1]

---

[1] A computer investigative specialist performed a review of the APPLE ICLOUD BACKUP DATA hard drive. Based on that review, a total of eleven Apple iPhone and iPad backups were identified within the APPLE ICLOUD BACKUP DATA. Of these, seven backups were determined to be non-pertinent device backups. Further, these non-pertinent seven backups appear to be outside the timeframe in question (prior to 2018) and/or device backups associated with other persons, i.e., Hallie Biden. The four remaining backups however, are all associated with Apple ID <rhbdc@icloud.com>, within the timeframe identified in the search warrant, and contained relevant materials.

15. In response to Apple Production 19275210, investigators sought authorization, which this Court granted in the summer of 2020, for a search warrant specifically for the APPLE ICLOUD BACKUP DATA for evidence of tax violations. *See* District of Delaware Case Number 20-165 M, issued on July 10, 2020.[2]

16. In searching the APPLE ICLOUD ACCOUNT and the APPLE ICLOUD BACKUP DATA, the government utilized keyword search terms and other protocols to help identify documents within the scope of the warrants. Based on this review, the government found evidence that was not only relevant to the ongoing tax investigation, including evidence related to the defendant's state of mind, but also evidence of other offenses, including the firearms offenses (hereafter the "SUBJECT OFFENSES") as further described in paragraph 22. This warrant seeks authorization to search the APPLE ICLOUD ACCOUNT and the APPLE ICLOUD BACKUP DATA for evidence of the firearms related SUBJECT OFFENSES described in paragraph 22.

B. MACBOOK PRO and EXTERNAL HARD DRIVE

17. Independently from the above-described search warrants related to the APPLE ICLOUD ACCOUNT and APPLE ICLOUD BACKUP DATA, investigators also obtained a MACBOOK PRO and an EXTERNAL HARD DRIVE in response to a grand jury subpoena.

---

[2] In the original search warrant obtained by the Internal Revenue Service (IRS), Delaware Case Number 20-165 M, signed on July 10, 2020, the Affiant denoted these four iCloud backups as Apple Backup 1, Apple Backup 2, Apple Backup 3, and Apple Backup 4. The backups were labeled 1 through 4 for purposes of the warrant and the affiant's description of the devices included the same device identifications included in this affidavit. In this instant warrant, your Affiant has numbered these same backup files as Apple Backup 1, Apple Backup 3, Apple Backup 4, and Apple Backup 11, which is how the files are labeled in the data maintained on law enforcement systems. This nomenclature is consistent with the original data provided by Apple.

18. This warrant would authorize the forensic examination of the MACBOOK PRO and the EXTERNAL HARD DRIVE for the purpose of identifying and seizing electronically stored data particularly described in Attachment B, specifically evidence of the SUBEJCT OFFENSES, which are firearms offenses more fully described in paragraph 22. Previously, the Court issued a search warrant for the MACBOOK PRO and the EXTERNAL HARD DRIVE that allowed the government to search for evidence of tax violations. *See* Delaware Case Number 19-309M issued on December 13, 2019.[3]

19. By way of background, on or about November 7, 2019, following a tip provided to law enforcement, FBI Special Agents interviewed Confidential Witness #1 (hereinafter "CW1"). CW1 is the owner of a computer store located in Wilmington, DE (hereinafter "Wilmington Computer Store"). The following is information provided by CW1 to law enforcement:

a. On or about April 12, 2019, HUNTER BIDEN brought three Apple brand laptop computers, including the MACBOOK PRO, to the Wilmington Computer Store for repair. According to CW1, HUNTER BIDEN was seeking to repair these computers and retrieve data from these computers because they were either damaged or malfunctioning. HUNTER BIDEN informed CW1 that the computers, including the MACBOOK PRO, belonged to him. CW1 inspected the computers to assess whether CW1 could repair and retrieve data from these computers. Based on this inspection, CW1 only retained the MACBOOK PRO for further repair and

---

[3] The Court also subsequently authorized a search warrant for the MACBOOK PRO and the EXTERNAL HARD DRIVE that allowed the government to search for evidence of Failure to Register as a Foreign Agent ("FARA") violations. *See* Delaware Case Number 20-214M issued on August 28, 2020.

data retrieval. Accordingly, CW1 returned the other two Apple computers back to HUNTER BIDEN and retained the MACBOOK PRO in CW1's possession at the Wilmington Computer Store for repairs. HUNTER BIDEN also provided a password to CW1 to access the MACBOOK PRO, even though CW1 did not require a password to access the data and complete the requested repairs.

b. On or about April 12, 2019, HUNTER BIDEN signed an invoice for the repair and recovery services for the MACBOOK PRO, which included a total labor cost of $85.00. Payment for the labor cost was due at the time the services were completed. The invoice also contained language that indicated if HUNTER BIDEN's computer equipment was left with the Wilmington Computer Store for a period of 90 days after HUNTER BIDEN was notified that services were completed, the equipment would be treated as abandoned and the Wilmington Computer Store would be held harmless for any damage or loss of the property. HUNTER BIDEN left a telephone number, [redacted] an email address, <rhbdc@icloud.com>, for CW1 to contact him when the repair services were complete.

c. Prior to starting any repairs on the MACBOOK PRO, CW1 requested that HUNTER BIDEN provide an external hard drive so that CW1 could back-up the data from the MACBOOK PRO to the external hard drive. On or about April 16, 2019, HUNTER BIDEN provided CW1 the EXTERNAL HARD DRIVE.

d. The data from the MACBOOK PRO could be accessed by CW1 while the computer was being repaired. As part of the repair service, CW1 created a backup file of the MACBOOK PRO's data, which was saved to the Wilmington Computer Store's server. According to CW1, backup files such as the file previously described are

typically retained for several weeks after the customer retrieves their device before being purged. This is done as a precautionary measure for the customer in the event that they are unable to access their data after their device is returned. CW1 also backed-up the data from the MACBOOK PRO onto the EXTERNAL HARD DRIVE.

e. On or about April 17, 2019, CW1 completed the computer repair and data recovery services for the MACBOOK PRO.

f. Between on or about April 17, 2019, and on or about April 24, 2019, CW1 made several attempts to notify HUNTER BIDEN that the repair and data recovery services for the MACBOOK PRO were complete and that payment was now due for these services. CW1 initially left a voicemail for the HUNTER BIDEN by calling the [redacted] telephone number provided by HUNTER BIDEN. CW1 next used an online billing application to submit a request for payment to HUNTER BIDEN. Finally, CW1 left another voicemail at the [redacted] provided by HUNTER BIDEN and sent another request for payment using the online billing application.

g. In or around late July 2019, CW1 became aware of media reports regarding HUNTER BIDEN and his connection to the country of Ukraine. CW1 accessed the Wilmington Computer Store's server and viewed certain portions of the backup data from the MACBOOK PRO, including emails sent to and from HUNTER BIDEN, between the years 2014-2019. At the time he did this, CW1 did not inform law enforcement that he accessed the data, nor was CW1 ordered, directed, or advised to do so by anyone, including any law enforcement officer.

h. CW1 viewed "hundreds" of emails between HUNTER BIDEN and other individuals. These emails related to a Ukrainian company on whose board HUNTER BIDEN sat, Burisma, as well as communications between HUNTER BIDEN and other individuals.

i. Based upon the emails viewed by CW1, CW1 became concerned about CW1's personal safety and the Wilmington Computer Store's reputation.

20. Based on information received from Apple, the MACBOOK PRO was registered to HUNTER BIDEN's Apple iCloud account on October 21, 2018, which utilized HUNTER BIDEN's email address of <rhbdc@icloud.com>. The MACBOOK PRO was also registered to the address [redacted] Wilmington, Delaware, and the phone number of [redacted] which I know are both associated with HUNTER BIDEN. The Barley Mill address is a location where HUNTER BIDEN has been known to periodically reside. The phone number [redacted] was previously registered in HUNTER BIDEN's name. The [redacted] telephone number and the <rhbdc@icloud.com> email address also match the contact information provided by HUNTER BIDEN to CW1 when he requested repair work for the MACBOOK PRO. The product was a Mac Book Pro 13.3 inches, space gray, 2.3 GHZ/8GB/256GB. Apple also provided a DSID of 436512608 for this device.

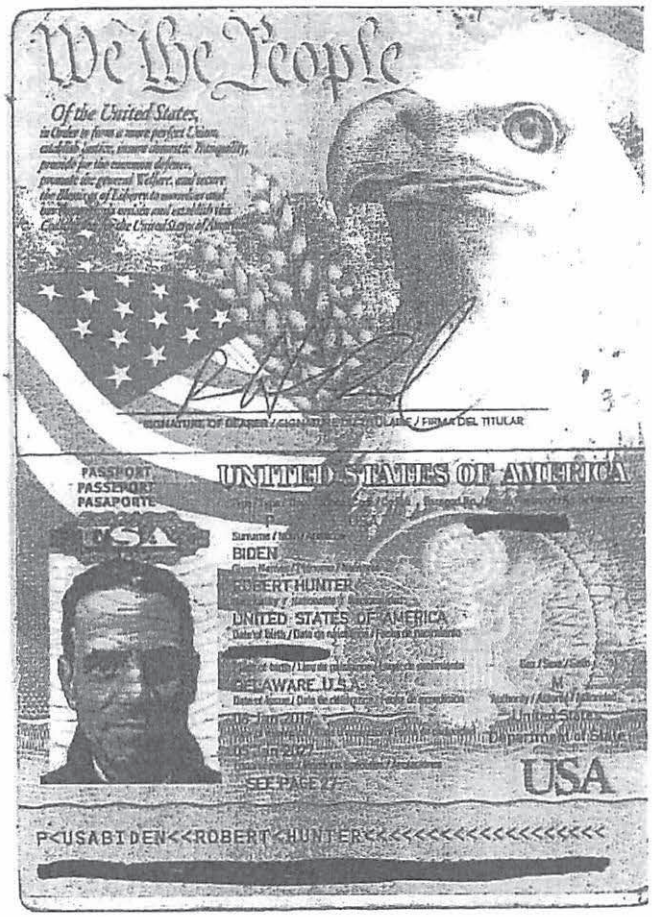
21. As stated above, the MACBOOK PRO and the EXTERNAL HARD DRIVE are currently in the lawful possession of the FBI. It came into the FBI's possession in the following way: On or about December 9, 2019, the United States Attorney's Office for the District of Delaware issued a grand jury subpoena to CW1 for the MACBOOK PRO and the EXTERNAL HARD DRIVE. CW1 also provided consent for law enforcement agents to seize the MACBOOK PRO and the EXTERNAL HARD DRIVE. Therefore, while law enforcement may already have

authority to examine the MACBOOK PRO and the EXTERNAL HARD DRIVE, your affiant seeks this warrant in order to obtain judicial authorization to search the MACBOOK PRO and the EXTERNAL HARD DRIVE for evidence of the SUBJECT OFFENSES, namely firearms offenses.

III. PROBABLE CAUSE

22. This warrant asserts there is probable cause to believe that HUNTER BIDEN has violated 18 U.S.C. §§ 922(a)(6) and 924(a)(2) related to making a false statement during a background check to deceive a firearms dealer, 18 U.S.C. § 924(a)(1)(A) related to making a false statement during a background check on records that the firearms dealer was required to maintain, and 18 U.S.C. §§ 922(g)(3) and 924(a)(2) related to his illegal possession of a Colt Cobra 38SPL revolver between October 12, 2018 and October 23, 2018 when HUNTER BIDEN was addicted to and an unlawful user of crack cocaine (these offenses are collectively referred to as the "SUBJECT OFFENSES" throughout this affidavit). On September 14, 2023, a grand jury returned a three-count indictment charging HUNTER BIDEN with the SUBJECT OFFENSES. On October 3, 2023, HUNTER BIDEN pled not guilty to each of the counts in the indictment.

23. Relevant to the probable cause for this warrant, on October 12, 2018, HUNTER BIDEN purchased a Colt Cobra Revolver bearing serial number RA551363 (hereinafter, "COLT COBRA") at StarQuest Shooters & Survival Supply store located in Wilmington, DE. In connection with the purchase, HUNTER BIDEN supplied his passport, a redacted copy of which is below:



24. During the purchase HUNTER BIDEN completed ATF Form 4473 (hereinafter "FORM 4473"). On FORM 4473, HUNTER BIDEN responded "NO" to question 11E asking, "Are you an unlawful user of, or addicted to, marijuana or any depressant, stimulant, narcotic drug, or any other controlled substance?"

25. There is probable cause to believe that HUNTER BIDEN was an unlawful user of, and addicted to a controlled substance, specifically crack cocaine, when he completed FORM 4473. The evidence of this includes, but is not limited, information provided by multiple witnesses and statements made by HUNTER BIDEN.

26. For example, HUNTER BIDEN authored a memoir, titled *Beautiful Things: A Memoir*. In chapter nine, titled "California Odyssey," HUNTER BIDEN wrote that his

"superpower" was "finding crack anytime, anywhere." HUNTER BIDEN further recounted his "five-month self-exile in Los-Angeles" beginning in the Spring of 2018 and wrote, "the amount of alcohol I consumed and crack I smoked was astounding – even death defying." Later HUNTER BIDEN described his experience checking into a rehab center in Brentwood and living with a sober coach off Nichols Canyon, "it was great – the beauty, the peace, the support – right up until the moment I relapsed."

27. [redacted] HUNTER BIDEN exchanged text messages with Elizabeth Secundy during the spring and summer of 2018. In one instance, on May 25, 2018, HUNTER BIDEN sent a text to Elizabeth Secundy stating "I finally have a chance to be the hero of my own story rather than the misunderstood addict that did so much but just never could live up to his potential."

28. Several months later, on July 23, 2018, HUNTER BIDEN sent a text to Secundy and said "So are we finished [with] you lecturing me that all of this hinges on my sobriety. Got it"

29. [redacted] your affiant is aware that in late August 2018, HUNTER BIDEN and a member of HUNTER BIDEN'S family sought and paid for detoxification and stabilization services at The View located in Brentwood, Los Angeles, California. Additional payments were made to Transcend Mentoring Inc., for a sober companion around the same period.

30. HUNTER BIDEN wrote in Chapter 10 of his memoir, "I returned that fall of 2018, after my most recent relapse in California, with the hope of getting clean through a new therapy and reconciling with Hallie. Neither happened."

31. [redacted] Hallie Biden, HUNTER BIDEN'S sister-in law, testified [redacted] regarding her relationship and interactions with the HUNTER

BIDEN in 2018. Hallie Biden testified that when HUNTER BIDEN stayed at her home during the summer of 2018, she would search HUNTER BIDEN's belongings for drugs and drug paraphernalia, which she found on multiple occasions. In late October 2018, Hallie Biden testified on one occasion she searched HUNTER BIDEN's belongings and located, [redacted]remnants, paraphernalia, and a gun in his car[redacted].

32. On February 15, 2022, Zoe Kestan, one of HUNTER BIDEN'S romantic partners, [redacted] testified before a Delaware federal grand jury. Kestan stayed with HUNTER BIDEN periodically from approximately April through August 2018 in California and testified about HUNTER BIDEN's crack cocaine use throughout that time period. Kestan testified that, "the drug, I mean, it was constant from the beginning, but it probably got even more constant, you know, to the amount that he was using by the second half of that stay."

33. Text messages [redacted] show that around this same time, HUNTER BIDEN sent a text to Kestan saying "You act as if Iwe didn't talk about addiction constantly I told on myself constantly I told you that you have to keep a distance and not feel responsible for me I told you that I would try as hard as I could and and that never asked for you to become codependant…"

34. Kestan visited HUNTER BIDEN in California in approximately September 2018. Kestan testified that HUNTER BIDEN appeared more "scattered" and that he was staying alone in a huge messy house, with frequent visits from strangers. Later that fall, Kestan visited HUNTER BIDEN in Massachusetts at a drug treatment facility. Despite being at a treatment facility, Kestan testified he was still smoking crack cocaine.

35. Financial records [redacted] show on November 29, 2018, HUNTER BIDEN's business made a $1,500 payment referencing Blue Water Wellness.

Blue Water Wellness, located in Newburyport, MA, advertised itself as a "healing place for the mind and body."

36. [redacted] Buhle is HUNTER BIDEN's ex-wife. Buhle and HUNTER BIDEN separated 2015 and later divorced in 2017. [redacted] during the period of their marriage, she periodically looked in vehicles driven by HUNTER BIDEN before her daughters drove those vehicles. On multiple occasions, BUHLE found what she believed to be narcotics, crack pipes, and other items indicating drug usage. On some occasions, these aforementioned items were observed in bags that belonged to HUNTER BIDEN.

37. The firearm described in paragraph 23 was recovered by law enforcement following a series of events in which Hallie Biden discovered the firearm in a vehicle utilized by HUNTER BIDEN and discarded the firearm in a trash receptacle behind a market in Delaware on or about October 23, 2018. An individual discovered this firearm with a brown colored pouch and law enforcement later recovered from that individual the firearm, brown colored pouch, ammunition, and items that HUNTER BIDEN had purchased from StarQuest Shooters. On the brown colored pouch, law enforcement observed a white/off-white solid residue adhered to the interior side of the flap and the bottom interior. Samples were collected from each area and combined for testing by a chemist at the FBI laboratory in Quantico, Virginia in September/October 2023. After running a series of tests, the chemist identified cocaine within the residue that was sampled and examined.

38. Based upon HUNTER BIDEN's memoir, [redacted] financial records, and other evidence reference above, there exists probable cause to believe HUNTER BIDEN was addicted to and an unlawful user of crack cocaine in 2018 and specifically, on October 12, 2018. Further, there is probable cause to believe that HUNTER BIDEN falsely stated that he was not

addicted to narcotics on FORM 4473. Through my training and experience, I am aware that such a representation is material to the purchase of a firearm because a firearms dealer is not permitted to sell a firearm to an individual who truthfully reports that they are addicted to a controlled substance at the time of purchase.

39. Through my training and experience, and through conversations with other law enforcement officers, your affiant is aware that drug users often maintain evidence of their addiction on their electronic devices. For instance, drug users use their electronic devices, including cellular phones, to arrange drug purchases through messaging, messaging applications, and phone conversations. Additionally, your affiant is aware that drug users often take photographs of their drug activity and save or send those items on communication devices and through Apple accounts. Your affiant believes the MACBOOK PRO, the EXTERNAL HARD DRIVE, the APPLE ICLOUD ACCOUNT and the APPLE ICLOUD BACKUP DATA contain communications and backups of data from phones and other electronic devices associated with HUNTER BIDEN, and as such, there exists probable cause that these devices contain evidence of his drug addiction and violations of firearms offenses described in Paragraph 22.

IV. BACKGROUND CONCERNING ELECTRONIC EVIDENCE AND DATA

A. APPLE ICLOUD ACCOUNT

40. In my training and experience, I have learned that Apple provides a variety of online services, including electronic mail ("email") access, to the public. Subscribers obtain an account by registering with Apple. During the registration process, Apple asks subscribers to provide basic personal information. Therefore, the computers of Apple are likely to contain stored electronic communications (including retrieved and unretrieved email for Apple subscribers) and information

concerning subscribers and their use of Apple services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. An Apple subscriber can also store with the provider files in addition to emails, such as address books, contacts or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Apple. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

42. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

43. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as

logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

44. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

45. This application seeks a warrant to search all responsive records and information under the control of Apple, a provider subject to the jurisdiction of this court, regardless of where Apple has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Apple's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

46. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement.

B. APPLE ICLOUD BACKUP DATA

47. This application seeks permission to search for communications, conversations, documents, photographs, and videos messages found in the APPLE ICLOUD BACKUP DATA which are located on the APPLE ICLOUD ACCOUNT. Your affiant believes that Apple previously produced these items in response to the search warrant for HUNTER BIDEN's Apple iCloud account because these backups are associated with his account.

48. There is probable cause to believe that this forensic electronic evidence might be on the APPLE ICLOUD BACKUP DATA because:

a. Data on the storage medium can provide evidence of a message that was once on the storage medium but has since been deleted or edited, or of a deleted portion of the message. Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a backup is evidence may depend on other information stored on the backup and the application of knowledge about how the backup behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the APPLE ICLOUD BACKUP DATA consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

g. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

C. MACBOOK PRO and EXTERNAL HARD DRIVE

49. As described above and in Attachment B, this application seeks permission to search for records that might be found on the MACBOOK PRO and the EXTERNAL HARD

DRIVE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, this warrant would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

50. I believe that things that were once stored on the MACBROOK PRO and the EXTERNAL HARD DRIVE may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system

configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

51. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the MACBROOK PRO and the EXTERNAL HARD DRIVE were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the MACBROOK PRO and the EXTERNAL HARD DRIVE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were

created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

52. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the MACBROOK PRO and the EXTERNAL HARD DRIVE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

53. As outlined above, the Court previously issued a search warrant for information associated with the email address and iCloud account <rhbc@icloud.com> that was stored at Apple, Inc., *see* District of Delaware Case Number 19-234 M, issued on August 29, 2019; a search warrant was authorized for the APPLE ICLOUD BACKUP DATA, *see* District of Delaware Case Number 20-165 M, issued on July 10, 2020; and a search warrant was authorized for the MACBOOK PRO and the EXTERNAL HARD DRIVE that allowed the government to search for evidence of tax violations, *see* Delaware Case Number 19-309M issued on December 13, 2019. As authorized in those warrants, a filter review process was followed to screen any privileged communications from being provided to the investigators. Specifically, the review was conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and other operative privileges because HUNTER BIDEN was a lawyer at the time of the conduct described in this warrant. Those procedures include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges. The filter review process was completed and only non-privileged items were provided to the investigative team. A filter review process is not necessary here because investigators will only search the evidence that has already been passed through the filter review process. Specifically, investigators will not execute this search warrant on the original data sets of evidence; rather, investigators will only review the evidence that has already been passed through the completed filter review process.

V. CONCLUSION

54. I submit that this affidavit supports probable cause for a search warrant authorizing

the examination of the items described in Attachment A to seize the items described in Attachment B.

VI. REQUEST FOR SEALING

55. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation and statements made by witnesses. Accordingly, there is good cause to seal these documents because their premature disclosure may cause third-parties to confront witnesses and may lead to obstruction of the investigation. Furthermore, your affiant believes there may be danger to witnesses who are disclosed publicly at this time.

Respectfully submitted,

[redacted]

Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on December 4, 2023:

Christopher J. Burke

THE HONORABLE CHRISTOPHER J. BURKE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. This warrant authorizes the forensic examination of the below described items for the purpose of identifying the electronically stored information described in Attachment B.

2. An APPLE ICLOUD ACCOUNT associated with <rhbdc@icloud.com> that was stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at 1 Infinite Loop, Cupertino, California, 95014, and is currently located at the FBI-Wilmington Resident Agency, 500 Delaware Avenue, Suite 300 Wilmington, Delaware, 19801.

3. APPLE ICLOUD BACKUP DATA located in the iCloud account data associated with <rhbdc@icloud.com> contained within Apple Production 19275210 received on or about September 25, 2019, pursuant to a prior search warrant for the Apple email account <rhbc@icloud.com>. The APPLE ICLOUD BACKUP DATA associated with <rhbdc@icloud.com> and that will be searched includes the following specific device information:

a. A backup of Apple iPhone X Device Identification D_8c78970d9dda9f5dbc1625b311efc72a6c50f68f ("Apple Backup 1");

b. A backup of Apple iPhone 6S Device Identification D_cdbe6900fc533da66a6c28169158d05cfb419a70 ("Apple Backup 3"); \

c. A backup of Apple iPad Pro Device Identification D_f846713a36c06653457179e18582aa1c478e8db4 ("Apple Backup 4");

d. A backup of Apple iPhone XR Device Identification D_a15b4a173b8ee009ee9adb908be74e4db618a323 ("Apple Backup 11").

(Collectively, the APPLE ICLOUD BACKUP DATA)

4. The APPLE ICLOUD BACKUP DATA is currently located at the FBI-

Wilmington Resident Agency, 500 Delaware Avenue, Suite 300, Wilmington, Delaware, 19801.

5. An (1) Apple MacBook Pro Laptop Computer; Serial Number FVFXC2MMHV29 ("MACBOOK PRO"); and (2) Western Digital External Hard Drive; Serial Number WX21A19ATFF3 ("EXTERNAL HARD DRIVE"). The MACBOOK PRO and the TARGET HARD DRIVE are currently located at the FBI-Wilmington Resident Agency, 500 Delaware Avenue, Suite 300, Wilmington, Delaware, 19801.

ATTACHMENT B

1. All records on the items described in Attachment A that are evidence of violations of 18 U.S.C. §§ 922(a)(6) and 924(a)(2) related to making a false statement during a background check to deceive a firearms dealer, violations of 18 U.S.C. § 924(a)(1)(A) related to making a false statement during a background check on records that the firearms dealer was required to maintain, and violations of 18 U.S.C. §§ 922(g)(3) and 924(a)(2) related to illegal possession of a firearm by Robert Hunter Biden, during the time period of January 1, 2018 to December 31, 2018, including:

   a. All evidence relating to addiction, substance use, and controlled substances, to include conversations, messages communications, photographs, documents, and videos.

   b. Evidence indicating the state of mind of the owner and user of the devices as it relates to the crime under investigation.

   c. Evidence of user attribution showing who used or owned the item at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

2. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.